Protection minimale de son environnement de travail

Avant Internet, les principales menaces étaient d'ordre « physiques » (pénétration dans des locaux informatiques sans autorisation, vol, vandalisme, incendies, dégâts des eaux ou panne électrique, insouciance et maladresse d'un employé). La situation est aujourd'hui différente puisque des agressions peuvent être menées via Internet sans la présence physique de l'agresseur.

Comme la mise en place de la protection d'un environnement de travail va dépendre du système informatique utilisé, nous allons traiter les 2 cas d'entreprise les plus représentatifs.

Cas 1 : L'entreprise Ganymède a un ou plusieurs postes de travail mais n'a pas de serveur.

Cas 2 : L'entreprise Encélade a un ou plusieurs postes de travail et dispose d'un serveur.

Cas 1 : l'entreprise Ganymède

Cas 1 : L'entreprise Ganymède a un ou plusieurs postes de travail mais n'a pas de serveur.

Facilité de mise en œuvre : Moyenne
Facilité d'exploitation : Moyenne
Hauteur de l'investissement humain : Moyen

Les règles que l'entreprise doit suivre :

- Equiper le site d'une alarme anti-intrusion.
- Brancher sur onduleurs ou sur circuit électrique ondulé tous les équipements informatiques, à savoir le routeur Internet, les switchs, les bornes wi-fi et les postes de travail.
- Placer le routeur Internet et les switch dans un endroit sécurisé et fermé à clé.
- Activer la fonction pare-feu sur le matériel permettant l'accès à interrnet (routeur, Livebox ou autres …)
- Installer les câbles réseaux dans des chemins de câbles, afin de les rendre invisibles et de mieux les protéger.
- Ne pas laisser connectées au réseau informatique les prises murales, qui ne sont pas utilisées, afin d'empêcher un branchement sans autorisation sur le réseau.
- Modifier les configurations et les mots de passe administrateur installés par défaut sur les routeurs d'accès à internet, les imprimantes réseaux et les switch, qui sont administrables.
- Fermer à clé les bureaux lorsque l'on est absent.
    - Eviter d'installer sur le réseau les PC portable des visiteurs. Ils peuvent par exemple être vérolés et infecter les postes de l'entreprise ou être utilisés pour récupérer des informations sensibles.

- Installer un PC en salle de réunion, qui serait dédié à toutes personnes ayant besoin d'accéder à Internet pour leurs démonstrations. Ce PC aurait comme particularité d'être sécurisé, d'être régulièrement audité et ne pourrait accéder qu'à internet.

- Eviter d'utiliser les clé USB et/ou CD /DVD extérieurs sans les contrôler au préalable par un antivirus et anti-spyware (anti-espion), à jour. Eux aussi peuvent être vérolés et infecter les postes.

- Ne jamais installer d'imprimante réseaux, Fax, photocopieur dans une zone accessible par toutes personnes extérieures à votre entreprise (par exemple hall ou zone d'attente ou de circulation).

- Demander le nettoyage des disques durs sur les équipements multifonctions, qui sont loués (imprimantes, Fax, photocopieurs) avant de les rendre. Vous éviterez ainsi le risque de voir des informations sensibles tomber dans les mains de personnes extérieures.

- Créer un profil pour vos stagiaires qui leur permet d'accéder aux seules données auxquels ils ont droit. Ce profil doit être désactivé et le mot de passe changé après leur départ.

- Installer un dispositif antivol sur les matériels les plus critiques.

Recommandations particulières pour les postes de travail.

- Ne jamais laisser des CD ou des disquettes de sauvegarde près des postes de travail. Ces CD ou disquettes doivent être stockées dans un lieu fermé et accessible que par des personnes bien déterminées.

- Ne pas laisser à proximité des post-it qui indiquent des mots de passe.

- Configurer les postes de travail, de telle sorte qu'ils ne démarrent pas à partir d'une disquette, d'un cd-rom ou d'une clé USB.

- Protéger par un mot de passe le setup c'est à dire le programme système du poste, afin d'empêcher toute modification non autorisée.

- Disposer les écrans, de telle sorte que l'on ne peut pas voir ce qui est affiché.

- Conditionner l'ouverture de session des PC par un login et un mot de passe fort. Ce mot de passe doit contenir 10 caractères composés de minuscules, majuscules, de chiffres et des symboles, afin de mieux résister aux utilitaires de découverte automatique. Il doit aussi être changé régulièrement.

- Conditionner aussi l'accès à vos logiciels métiers par login et mot de passe.

- Utiliser CTRL+ALT+SUPPR, afin de verrouiller les postes de travail lors des absences du bureau ou automatiser le lancement de la mise en veille du poste, après un délai d'inactivité. Le poste de travail ne pourra être relancé qu'après saisie du mot de passe.

- Ne pas utiliser le compte Administrateur mais des profils utilisateurs avec des droits limités pour l'utilisation habituelle des Postes de travail.

- Renforcer la protection des comptes Administrateur et Invité :

  - en les renommant et en leur attribuant des mots de passe forts.

  - en remplaçant les description des comptes par autre chose que le texte par défaut, afin d'empêcher

une identification trop facile.

- et en vérifiant que le compte invité est bien désactivé.

- Protéger la base de registre contre tout accès anonyme.

- Désactiver le stockage des mots de passe faibles.
  Cf http://www.securite-informatique.gouv.fr/gp_article193.html

  - Désactiver les services qui ne sont pas indispensables et dangereux comme l'Album, le Partage de connexion Internet (ICS), Messenger, NetMeeting, le Gestionnaire de connexion automatique d'accès client.

  - Désactiver l'assistance et le bureau à distance, c'est à dire l'utilitaire de prise de contrôle à distance Windows et ne le réactiver que lorsque vous en avez besoin.

- Installer une solution complète de sécurité (antivirus- antispyware/anti-espion) toujours à jour et active, couplée à un pare-feu.

- Programmer un contrôle antiviral, antispyware (anti-espion) hebdomadaire.

- Automatiser la mise à jour des derniers services Packs et des correctifs de sécurité du système et des logiciels de sécurité (pare-feu, antivirus).

- Protéger les fichiers, répertoires et disque dur partagés :

  - en enlevant tous les partages non utilisés.

  - en masquant les partages, afin de les rendre inaccessibles aux personnes étrangères à l'entreprise (le nom de partage doit se terminer par un $).

  - en n'affectant le partage et les permissions qu'aux utilisateurs autorisés, et en enlevant entre autre le compte « Tout le monde ».

Cas 2: l'entreprise Encélade

L'entreprise Encélade a un ou plusieurs postes de travail et dispose d'un serveur

Facilité de mise en œuvre : difficile
Facilité d'exploitation : difficile
Hauteur de l'investissement humain : forte

Les règles, que l'entreprise doit suivre :

- Equiper le site d'une alarme anti-intrusion.

- Disposer d'un local, toujours fermé à clé, qui regroupe les éléments informatiques et telecom vitaux du

Système informatique, tels que les points d'accès externes (téléphone, Internet, liaisons louées), les armoires de brassage informatique, l'autocom, les routeurs, les commutateurs, les bornes wi-fi et les serveurs.

- Ce local doit être climatisé et éloigné des canalisations d'eau et des sanitaires. Son circuit électrique doit être spécifique, régulé et équilibré (ondulé).

- Ne pas utiliser le local informatique à d'autres usages (matériaux déclassés, cartons, papier, local de rangement pour le ménage).

- Décomposer le site en plusieurs zones d'accès de plus en plus strictes jusqu'au local informatique. Il sera ainsi plus facile de contrôler les allers et venus des personnes extérieures.

- Installer un dispositif antivol sur les matériels les plus critiques.

- Ne jamais installer d'imprimante réseaux, Fax, photocopieur dans une zone accessible par toutes personnes extérieures à votre entreprise (par exemple hall ou zone d'attente ou de circulation).

- Demander le nettoyage des disques durs sur les équipements multifonctions, qui sont loués (imprimantes, Fax, photocopieurs) avant de les rendre. Vous éviterez ainsi le risque de voir des informations sensibles tomber dans les mains de personnes extérieures.

- Formaliser des règles précises pour les visiteurs (clients, fournisseurs, presse) comme :

  - personne ne doit pouvoir rentrer dans les locaux sans autorisation.

  - Aucun PC portable extérieur ne doit être installé sur le réseau. Ils peuvent par exemple être vérolés et infecter les postes de l'entreprise ou être utilisés pour récupérer des informations sensibles.

  - aucune clé USB et/ou DVD extérieur ne doit être utilisé sur un Poste de travail sans avoir été contrôlé au préalable par un antivirus - antispyware (anti-espion). Eux aussi peuvent être vérolés et infecter les postes.

    - Installer par exemple un PC en salle de réunion, qui serait dédié à toutes personnes ayant besoin d'accéder à Internet pour leurs démonstrations. Ce PC aurait comme particularité d'être sécurisé, d'être régulièrement audité et ne pourrait accéder qu'à internet.

    - Fermer à clés les bureaux lorsque l'on est absent.

- Installer les câbles réseaux dans des chemins de câbles, afin de les rendre invisibles et de mieux les protéger.

- Ne pas laisser connectées au réseau informatique les prises murales, qui ne sont pas utilisées, afin d'empêcher un branchement sans autorisation sur le réseau.

- Modifier les configurations et les mots de passe administrateur installés par défaut sur le routeur internet, les imprimantes réseaux, les bornes wi-fi et les switch, qui peuvent être administrables.

- Disposer d'un switch de dépannage.

- Installer un pare-feu, afin de protéger votre entreprise des intrusions extérieures.

- Cloisonner le réseau interne en plusieurs sous – réseaux, afin de séparer par exemple la direction des

autres services et de mieux se protéger contre la propagation d'une infection.

- Utiliser comme mot de passe pour l'accès aux différentes parties de son informatique, des mots de passe forts, qui peuvent mieux résister aux utilitaires de découverte automatique. On entend par mot de passe fort, des mots de passe longs (10 caractères au moins) composés de minuscules, majuscules, de chiffres et de symboles.

- Obliger l'utilisation et le changement régulier de mots de passe forts utilisateurs:

  - en recourant aux objets de stratégie de groupe (GPO) sur un serveur Windows, qui permet d'appliquer des règles de sécurité centralisées.

  ou

  - en utilisant PAM sur un serveur Linux, qui est un module d'authentification et de gestion des accès. Il permet, entre autre, de définir des règles strictes dans l'utilisation des mots de passe utilisateurs.

- Utiliser des profils utilisateurs avec des droits limités et brider leur environnement de travail par le biais des stratégies de groupes (GPO). De cette façon, il sera possible par exemple, de masquer le voisinage réseau ou d'interdire l'installation d'écran de veille ou d'images, qui peuvent être vecteur de programmes malveillant.

  1. Créer un profil pour les stagiaires qui leur permet d'accéder aux seules données auxquels ils ont droit. Ce profil doit être désactivé et le mot de passe changé après leur départ.

Recommandations particulières pour le serveur.

- ne jamais laisser les disquettes de boot ou CD en libre accès près du serveur.

- le configurer de telle sorte qu'il ne démarre pas à partir d'une disquette, d'un cd-rom ou d'une clé USB.

- Protéger, par un mot de passe, le setup c'est à dire le programme système du poste, afin d'empêcher toute modification non autorisée.

- le protéger par un onduleur assez récent, qui dispose de l'option shutdown. Cette option permet d'éteindre proprement le serveur, après une coupure électrique d'une certaine durée.

- l'alimentation doit être réalisée par des modules connectables à chaud et redondants

- les connexions réseaux doivent être doublées.

- la prise en charge des disques hot-plug (remplaçables à chaud) et la mise en place du RAID, doivent être disponibles, afin de garantir une disponibilité plus importante.

- le protéger par un antivol (marquage – tatouage - câble).

- la fermeture de l'unité centrale avec un cadenas doit être possible.

- verrouiller l'écran par un mot de passe et l'éteindre.
- ne pas laisser à proximité les post-it, qui indiquent les mots de passe.
- installer une solution complète de sécurité (antivirus – antispyware / anti-espion) toujours à jour et active.
- programmer un contrôle antiviral, antispyware hebdomadaire.

- Automatiser la mise à jour des derniers services Packs et des correctifs de sécurité du système et des logiciels de sécurité (pare-feu, antivirus).
  - protéger le serveur par un pare-feu applicatif ou cloisonner votre réseau de telle sorte que tous les flux en provenance ou en direction du serveur soient contrôlés et filtrés.
  - Sécuriser les comptes Administrateur et Invité :
    - en les renommant et en leur attribuant des mots de passe longs et complexes.
    - en remplaçant les description des comptes par autre chose que le texte par défaut, afin d'empêcher une identification trop facile.
    - en vérifiant que le compte invité est bien désactivé.
    - et en enregistrant ces modifications dans un endroit sûr
  - Désactiver les autres comptes systèmes inutilisés et leur affecter un mot de passe long et complexe.
  - protéger le registre contre tout accès anonyme et supprimer la possibilité d'y accéder à distance.
  - ne laisser ouverts que les seuls services qui sont nécessaires au fonctionnement de vos applications. Pensez à désactiver : Messenger, le service Fax, le Bureau à distance, Telnet, IIS, FTP, NTP, SMTP, POP.
  - protéger les fichiers, répertoires et disque dur partagés en n'affectant le partage et les permissions NTFS qu'aux utilisateurs autorisés et en enlevant impérativement le compte « Tout le monde ».
  - enlever aussi tous les partages non utilisés.

Recommandations particulières pour les postes de travail.

- Protéger les PC par un onduleur.
- Ne jamais laisser des CD ou des disquettes de sauvegarde près des postes de travail. Ces CD ou disquettes doivent être stockées dans un lieu fermé et accessible que par des personnes bien déterminées.
- Ne pas laisser à proximité des post-it qui indiquent des mots de passe.
- Configurer les postes de travail, de telle sorte qu'ils ne démarrent pas à partir d'une disquette, d'un cd-rom ou d'une clé USB.
- Protéger, par un mot de passe, le setup c'est à dire le programme système du poste, afin d'empêcher

toute modification non autorisée.

- Disposer les écrans, de telle sorte que l'on ne peut pas voir ce qui est affiché.

- Utiliser CTRL+ALT+SUPPR, afin de verrouiller les postes de travail lors des absences du bureau ou automatiser le lancement de la mise en veille du poste, après un délai d'inactivité. Le poste de travail ne pourra être relancé qu'après saisie du mot de passe.

- Renforcer la protection des comptes Administrateur et Invité :

  - en les renommant et en leur attribuant des mots de passe forts.

  - en remplaçant les description des comptes par autre chose que le texte par défaut, afin d'empêcher une identification trop facile.

  - et en vérifiant que le compte invité est bien désactivé.

- Protéger la base de registre contre tout accès anonyme.

- Désactiver le stockage des mots de passe faibles.
  Cf http://www.securite-informatique.gouv.fr/gp_article193.html

  - Désactiver les services qui ne sont pas indispensables et dangereux comme l'Album, le Partage de connexion Internet (ICS), Messenger, NetMeeting, le Gestionnaire de connexion automatique d'accès client.

  - Désactiver l'assistance et le bureau à distance, c'est à dire. l'utilitaire de prise de contrôle Windows et ne le réactiver que lorsque vous en avez besoin.

- Installer une solution complète de sécurité (antivirus- antispyware/anti-espion) toujours à jour et active, couplée à un pare-feu.

- Programmer un contrôle antiviral, antispyware (anti-espion) hebdomadaire.

- Automatiser la mise à jour des derniers services Packs et des correctifs de sécurité du système et des logiciels de sécurité (pare-feu, antivirus).

- Protéger les fichiers, répertoires et disque dur partagés :

  - en enlevant tous les partages non utilisés.

  - en masquant les partages, afin de les rendre inaccessibles aux personnes étrangères à l'entreprise (le nom de partage doit se terminer par un $).

  - en n'affectant le partage et les permissions qu'aux utilisateurs autorisés, et en enlevant entre autre le compte « Tout le monde ».